IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of
WATT et al
Serial No. 10/714,483
Filed: November 17, 2003

Confirmation No.: 6434
Atty. Ref.: 550-471
Group: 2183
Examiner: B. Johnson

For: MONITORING CONTROL FOR MULTI-DOMAIN PROCESSORS

* *

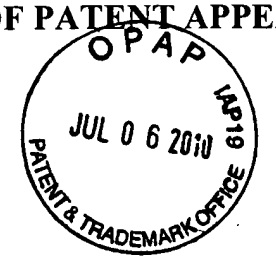
APPEAL BRIEF

On Appeal From Group Art Unit 2183

Stanley C. Spooner
NIXON & VANDERHYE P.C.
11th Floor, 901 North Glebe Road
Arlington, Virginia 22203
(703) 816-4028
Attorney for Appellant

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES



In re Patent Application of
WATT et al
Serial No. 10/714,483
Filed: November 17, 2003
For: MONITORING CONTROL FOR MULTI-DOMAIN PROCESSORS

Atty. Ref.: 550-471
Group: 2183
Examiner: B. Johnson

* *

July 6, 2010

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

I. REAL PARTY IN INTEREST

The real party in interest in the above-identified appeal is ARM Limited by virtue of an assignment of rights from the inventors to ARM Limited recorded August 20, 2004 at Reel 15714, Frame 905.

II. RELATED APPEALS AND INTERFERENCES

It is noted that a previous appeal to the Board of Patent Appeals and Interferences resulted in a Decision mailed March 31, 2009 in which the previous rejections of the claims were upheld by the Board. A Request for Continued

Examination and an amendment of the claims followed and, other than the Pre-Appeal Brief Request for Review previously filed in this current appeal, there are believed to be no related appeals, interferences or judicial proceedings with respect to the present application.

III. STATUS OF CLAIMS

Claims 1, 2, 4-21 and 23-39 stand rejected under 35 USC §103 over Alverson (U.S. Patent 7,020,767) in view of Angelo (U.S. Patent 6,581,162), either by itself or in view of "common art."

Claims 3 and 22 have been cancelled without prejudice.

The Examiner contends in the Final Rejection that claims 1, 2, 4-21 and 23-39 are rejected under 35 USC §112 (first paragraph) but this rejection was withdrawn on June 3, 2010 in view of the "Interview Summary" mailed by the Examiner on that date.

The above rejections of claims 1, 2, 4-21 and 23-39 are appealed.

IV. STATUS OF AMENDMENTS

No further response has been submitted with respect to the Final Official Action in this application other than the filing of a Pre-Appeal Brief Request for Review, which decision was mailed June 3, 2010 (Paper No. 20100601).

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' specification and figures provide an explanation of the claimed invention set out in independent claims 1 and 20, with each claimed structure and method step addressed as to its location in the specification and if illustrated in the figures.

"1. A method of controlling a monitoring function of a processor [10 as shown in figure 1 and discussed on page 15, line 8 to page 17, line 10 and elsewhere in the specification], said processor being operable in at least two domains [secure and non-secure as shown in Figure 2 and discussed on page 17, lines 12-30 and elsewhere in the specification], comprising a first domain and a second domain, said first and second domains each comprising at least one mode [non-secure mode applications 522 and 524 and secure mode applications 512, 514, 516 shown in Fig. 59 and also Figure 2 discussed on page 104, line 30 – page 105, line 2 and page 106, line 15 to page 107, line 11 and elsewhere in the specification], said method comprising the steps of:

controllably monitoring said processor operating in each of said at least two domains [discussion with respect to Fig. 59 on page 106, line 24 to page 109, line 24 and elsewhere in the specification],

setting at least one control value to an enable value, said at least one control value relating to a condition, said condition consisting of a respective one of (a) a domain that said processor is operating in [secure debug and trace enable bits as shown in Figure 61 and discussed a page, or (b) a mode that said processor is operating in or (c) a type of said monitoring function, said control value being set to be an enable value for said related condition to indicate that said monitoring function is allowable in said first domain [discussion with respect to Figs. 61 & 67 on page 109, lines 1-24 and elsewhere in the specification];

allowing initiation of said monitoring function in said first domain when said condition is present if its related control value is set to said enable value and thereby indicates that said monitoring function is allowable [discussion with respect to Figures 61 and 68 on page 109, lines 9-16, page 112, line 30 to page 113, line 16 and elsewhere in the specification]; and

not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value is not set to said enable value and thereby indicates that said monitoring function is not allowable [discussion with respect to Figures 61 and 68 on page 109, lines 9-16, page 112, line 30 to page 113, line 16 and elsewhere in the specification]."

"20. A processor [10 as shown in figure 1 and discussed on page 15, line 8 to page 17, line 10 and elsewhere in the specification] operable in a first domain and a second domain [secure and non-secure as shown in Figure 2 and discussed on page 17, lines 12-30 and elsewhere in the specification] said first and second domains each comprising at least one mode [non-secure mode applications 522 and 524 and secure mode applications 512, 514, 516 shown in Fig. 59 and also Figure 2 discussed on page 104, line 30 – page 105, line 2 and page 106, line 15 to page 107, line 11 and elsewhere in the specification], said processor comprising:

monitoring logic for controllably monitoring said processor operating in each of said first and second domains [ETM 22 and JTAG controller 18 as shown in Figure 1 and discussed on page 15, lines 8-30 and Figure 59 and discussed on page 106, line 24 to page 109, line 24 and elsewhere in the specification];

a storage element [CP14 as shown in Figures 67 and 68 and discussed on page 109, lines 1-24 and elsewhere in the specification] configured to be set to contain at least one control value, said at least one control value relating to a condition, said condition consisting of a respective one of (a) a domain that said processor is operating in, or (b) a mode that said processor is operating in or (c) a type of said monitoring function, said control value comprising an enable value for said related condition, said enable value indicating that operation of said monitoring logic is allowable in said first domain; and

control logic [620 as shown in Fig. 68 and discussed on page 112, line 30 – page 113, line 16 and elsewhere in the specification] configured to control initiation of said monitoring logic and for allowing initiation of said monitoring logic in said first domain when said condition is present if its related control value is set to said enable value and thereby indicates that operation of said monitoring logic is allowable, and for not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value is not set to said enable value and thereby indicates that operation of said monitoring logic is not allowable [as shown in Figures 61 and 68 and discussed on page 109, lines 9-16, page 112, line 30 to page 113, line 16 and elsewhere in the specification]."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, 4-8, 11-18, 20, 21, 23-36, 38 and 39 stand rejected under 35 USC §103 as unpatentable over Alverson (U.S. Patent 7,020,767) in view of Angelo (U.S. Patent 6,581,162).

Claims 9, 10, 19 and 37 stand rejected under 35 USC §103 as unpatentable over Alverson/Angelo "in view of common art."

Claims 1, 2, 4-21 and 23-39 stand rejected under 35 USC §112 (first paragraph) as failing to comply with the written description requirement in the

Final Rejection. This rejection has apparently been withdrawn by the Examiner pursuant to the communication mailed June 3, 2010 (Paper No. 20100601-A).

VII. ARGUMENT

Appellants' arguments include the fact that the burden is on the Examiner to first and foremost properly construe the language of the claims to determine what structure and/or method steps are covered by that claim. After proper construction of the claim language, the burden is also on the Examiner to demonstrate where a single reference (in the case of anticipation) or a plurality of references (in the case of an obviousness rejection) teaches each of the structures and/or method steps recited in independent claims 1 and 20.

Furthermore, the Court of Appeals for the Federal Circuit has stated in the case of *In re Rouffet*, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998)

> to prevent the use of hindsight based on the invention to defeat patentability of the invention, this court **requires** the examiner to show a **motivation** to combine the references that create the case of obviousness. In other words, the Examiner **must show reasons** that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. (Emphasis added).

In its recent decision, the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (April 2007), held that it is often necessary for a

court to look to interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace and the background knowledge possessed by a person of ordinary skill in the art in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. The Supreme Court held that "[t]o facilitate review, this analysis should be made explicit." *Id.* at 1396.

The Supreme Court in its *KSR* decision went on to say that it followed the Court of Appeals for the Federal Circuit's advice that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" (the Supreme Court quoting from the Court of Appeals for the Federal Circuit in *In re Kahn*, 78 USPQ2d 1329 (Fed. Cir. 2006)).

A. Correction of the Record

Appellants are in receipt of an "Interview Summary" mailed by the PTO on June 3, 2010. However, no interview was conducted by Examiner Faherty on or about June 1, 2010 as erroneously reported in the Interview Summary form. In fact, the undersigned firm has no record of receiving any call from Examiner Faherty on or about June 1, 2010.

Appellants have received both a Decision of the Pre-Appeal Panel and a purported Interview Summary dated June 3, 2010. The purported "Interview

Summary" impliedly suggests that Examiner Faherty conducted an interview with Appellants' undersigned representative on June 1, 2010. While Appellants' undersigned representative was in his office from approximately 7:00 AM until 3:00 PM, Appellants' representative can certify that the Examiner did not contact the undersigned. Moreover, neither Appellants' representative's secretary or the law firm receptionist have reported that Examiner Faherty had called (at least one of Appellants' secretary and/or receptionist would have been present in the office at all times until approximately 6:00 PM).

In view of the above, the Examiner's purported "Interview Summary" and his indication that an interview was conducted on June 1, 2010 is incorrect and the correction to the record is requested.

The notification that, in response to the Error #1 noted in the Supporting Statement for the Pre-Appeal Brief Request for Review, i.e., that the Examiner fails to support his §112 (first paragraph) rejection, was accepted by the Pre-Appeal Panel (and that the Examiner withdraws his unsupported rejection) is very much appreciated. However, it is requested that the record be corrected to confirm that at no time on June 1, 2010 was any interview with Examiner Faherty conducted.

B. The Examiner's definition of "control value relating to a condition" is inconsistent with the Board's Decision of March 31, 2009

While the Board agreed with the Examiner's broad construction of the claim term "control value" (prior to the current amendment), the Board did not agree with the Examiner's assertions as to what was disclosed in the cited prior art references. Specifically, the Board defined "condition" as being virtually anything taught by the prior art references (see Decision pages 7 and 8) and subsequently concluded that Angelo's (U.S. Patent 6,581,162) teaching of a "system request" met the unlimited but claimed "control value relating to a condition." (See the paragraph bridging pages 8 and 9 of the Decision).

As the Board reiterated its broad construction of "control value" and the previously unlimited "condition" (Decision, first full paragraph on page 9), the Examiner apparently concludes that the "control value" and the more limited "condition" as set out in current claims 1 & 20 is still disclosed in the cited prior art.

Appellants have amended independent claims 1 and 20 to limit the definition to three embodiments disclosed in the specification and specifically state that "said condition consisting of a respective one of (a) a domain that said processor is operating in, or (b) a mode that said processor is operating in or (c) a type of said monitoring function . . . ." Appellants previously made of record page 762 from *Webster's Ninth New Collegiate Dictionary* which defines "mode,"

especially in conjunction with computers, as "a particular functioning arrangement or condition: STATUS <a spacecraft in reentry ~> <a computer operating in parallel ~>."

The Examiner is believed to be defining the term "mode" in a manner different from the ordinary dictionary definition of the word (which dictionary definition is consistent with the manner in which the term is used in Appellants' specification and claims). There is nothing in any definition of "mode" in the computer field that indicates that it can be a "control value" or some other active operating function in a computer. It is simply a designation of a particular "functioning arrangement or condition" of the computer.

The Examiner is obligated to construe "mode" in the manner defined in the above dictionary definition, as used in the specification and in the manner well known to those of ordinary skill in the computer art, i.e., the attached definition of the term (all of which are consistent) which is different from any control value.

C. The Examiner fails to meet his burden of coming forward with evidence that Alverson or Angelo teach any control value relating to a condition where that condition is (a) a domain, (b) a mode, or (c) a type of monitoring function – therefore no *prima facie* case of obviousness under 35 USC §103

Beginning on page 3, section 6 of the outstanding Final Rejection, the Examiner rejects claims 1, 2, 4-8, 11-18, 20, 21, 23-36, 38 and 39 under 35 USC §103 as unpatentable over Alverson in view of Angelo.

With the previously unlimited claim 1, the Board held that "one of the 'conditions' taught by Angelo is a system request" and "a system request, . . . , subsequently generates an interrupt (asserts the SMI) and enters the system into SM mode (FF 12)." Applying the Board's analysis, the purported "control value" is the "SMI" of Angelo (as interpreted by the Board, Decision page 8 last full paragraph). The Angelo reference does not disclose a "mode." In fact, in Angelo, the purported "control value" is an "interrupt" and an interrupt is clearly not a "mode" that the processor is operating in (nor does it meet the definition of "mode"). An "interrupt," by its nature, is a request to change the manner in which the processor is operating but is not an indication of the "mode."

Moreover, because Appellants have limited the independent claims' definition of "condition" to one of the three specific options set out in the independent claims, the Board's (and the Examiner's previous) extremely broad interpretation of "condition" can no longer apply. Thus, the Board cannot conclude that the term "condition" can be met by the Angelo "system request" because a system request is neither "(a) a respective one of a domain that said processing is operating in **or** (b) a mode that said processing is operating in **or** (c) a type of said monitoring function . . . ." In view of the more limited nature of the current claim definition of "condition," the Angelo reference and its "system request" does not meet the current claim limitations.

Absent a specific teaching of where the currently amended claim limitations are taught anywhere in the Alverson/Angelo combination, the Examiner fails to meet his burden of setting out a *prima facie* case of obviousness for independent claims 1 and 20 or claims dependent thereon.

D. The Examiner's Final Rejection is vague and non-specific

It has been previously noted (in the amendment filed October 29, 2009, pages 13-14) that the Examiner previously cited large portions of the Angelo reference as purportedly teaching the claimed subject matter, but without identifying what portions he contends are the claimed subject matter. It is unclear as to whether the Examiner is maintaining his previous interpretation of this reference.

The Examiner's current interpretation of the Angelo reference is inconsistent with the Board's construction of the "SMI" in Angelo and its definition of "condition" as being a "system request." Accordingly, the Examiner's rejection is now believed to be completely unsupported by the Board of Patent Appeals and Interferences Decision and reconsideration is requested.

E. The Examiner fails to provide the required "analysis" of reasons for combining the references and therefore fails to meet his obligation of evidencing a *prima facie* case of obviousness

In view of the more limited definition of "condition," the Examiner fails to provide the Supreme Court's required "analysis" as to his reasons for combining Alverson and Angelo in a manner that would disclose the claimed "condition."

Even if the Examiner met his burden of showing where each and every claim limitation is shown in the Alverson/Angelo combination (and, as noted above, his vague and indefinite references do not meet this burden of the first prong of a *prima facie* case), the Examiner fails to meet the second prong of the minimum requirements of a *prima facie* case of obviousness as imposed by the Supreme Court in the *KSR* decision.

Accordingly, there is no *prima facie* case of obviousness.

F. The Examiner fails to set out an evidentiary basis for a rejection of claims 1, 2, 4-21 and 23-39 under the provisions of 35 USC §103(a)

In order to meet his burden of establishing a *prima facie* case of obviousness, the Examiner must identify evidence supporting the two prongs required for an obviousness rejection. The first prong is identifying evidence which shows that each claimed element or each claimed method step is present somewhere in the combination of references along with any claimed interrelationship. Even if the Examiner can show the first prong, the second prong

must be met, i.e., the Examiner is obligated under the Supreme Court ruling in *KSR* to provide an explicit "analysis" of how and why he picks and chooses individual elements or method steps from the various references and then combines them in the manner of Appellants' claims. As will be seen, neither of these are proven by the evidence of record.

1. The Examiner fails to identify all claimed elements and interrelationships

The Examiner fails to establish a *prima facie* case of obviousness because he does not disclose where or how the Alverson or Angelo references teach Appellants' claimed condition.

As noted in argument C above, the Examiner fails to identify any evidence suggesting that Appellants' claim now is directed to one of the three conditions specified ("said condition consisting of . . . ."). Quite clearly, as noted above, the purported "control value" in Angelo is an "interrupt" and not a "mode." The definition of "mode" as previously discussed is well known to those of ordinary skill in the art and this definition is supported by the evidence of record, i.e., page 762 from *Webster's Ninth New Collegiate Dictionary*. So there is no disclosure of the "mode" let alone the "domain" or the "monitoring function" as set out in claims 1 & 20.

Further, the Board's previously broad interpretation of "condition" no longer applies as Appellants' claim has been amended to limit the term to one of three

options discussed above. None of these three features is disclosed in the Angelo or Alverson reference. Because the Examiner fails to indicate where either Alverson or Angelo teaches any one of the three recited "conditions" required by Appellants' independent claims 1 and 20, all claimed structures are not disclosed in the Alverson/Angelo combination.

Again, the burden of establishing a *prima facie* case of obviousness is on the Examiner. Appellants do not have to prove a negative, i.e., that there is no disclosure in these two references. Appellants merely point out that the Examiner has failed to identify where any of the three claimed "conditions" are disclosed in the Alverson/Angelo combination. Accordingly, because the Examiner has failed to meet his burden of going forward with evidence showing that at least one of these three "conditions" is disclosed in the Alverson/Angelo combination, the Examiner has failed to set out a *prima facie* case of obviousness and no further proof of the Examiner's failure by Appellants is required.

Reviewing the Final Rejection in section 7, pages 3 and 4, it is clear that while the Examiner alleges that the three "conditions" are disclosed in Angelo, column 7, line 61 to column 8, line 4, the Examiner apparently again relies upon the same disclosure in Angelo which the Board held taught the unlimited "condition" in its Decision.

Appellants have now amended the independent claims to cover a more limited "condition" but the Examiner has failed to amend his arguments to indicate

how or where this currently claimed and more limited "condition" is disclosed in the cited prior art.

In view of the above, the rejection under 35 USC §103 with respect to the Alverson/Angelo combination is respectfully traversed.

2. The Examiner provides no proper "analysis" of his reasons for picking and choosing elements from the prior art and combining them in the manner of Appellants' claims

As noted above in the *KSR* case, the Supreme Court requires that the Examiner provide some explicit "analysis" as to why one of ordinary skill in the art would want to pick and choose elements from the various prior art references and then combine them in the manner of Appellants' claims.

Regarding claim 1, the Examiner in section 7 on pages 3 and 4 of the Final Rejection only makes the statement that "[i]t would have been obvious at the time of the invention for one of ordinary skill in the art to take the system of Alverson and incorporate the SMM and SMI security of Angelo." This conclusory statement ignores the Supreme Court requirement that the "analysis" be something **more** than a "conclusory statement."

Moreover, the Examiner ignores the additional limitations contained in Appellants' independent claim 1, i.e., that the "condition" be more specifically construed. The subsequent discussion on page 3 carrying over to page 4 of the Final Rejection merely comprises the Examiner's previous arguments as to where the

claimed elements are disclosed in the Alverson/Angelo combination, but does not address any reason for picking and choosing portions of the Alverson and Angelo references and then combining them in a manner of Appellants' independent claims 1 and 20 (assuming for the purpose of argument that those elements and/or method steps are actually disclosed somewhere in Alverson and Angelo).

The Examiner's failure to meet his burden of proof as to an explicit analysis as to why one would pick and choose elements from the combination of prior art references and then combine them in the manner of Appellants' claims confirms that the Examiner has failed to meet his second burden of establishing a *prima facie* case of obviousness. In view of the above, even if the three claimed "conditions" were disclosed somewhere in the prior art, the rejection of claims 1, 2, 4-21 and 23-39 would fail.

In view of the above, it is clear that the Examiner has failed to meet either prong of establishing a *prima facie* case of obviousness of the independent claims 1 and 20 over the Alverson/Angelo combination, whether applied by itself to claims 1, 2, 4-8, 11-18, 20, 21, 23-36 and 38-39 or in combination with the purported "common art" to reject claims 9, 10, 19 and 37. The failure of the Alverson/Angelo combination to disclose or render obvious the claimed features as well as the lack of any analysis for combining these two references clearly establishes the Examiner's

failure to meet his burden of proving a *prima facie* case of obviousness and therefore both rejections under 35 USC §103 are respectfully traversed.

VIII. CONCLUSION

The Examiner has apparently withdraw his section 112 rejection. The Examiner fails to adopt the Board's definition of a "control value relating to a condition" and clearly fails to demonstrate where the more narrowly claimed "condition" is disclosed anywhere in the combination of references. The Examiner's vague and indefinite references to Alverson and Angelo do not specifically identify where he contends the prior art discloses any of the three specifically claimed "conditions," i.e., (a) the "domain", (b) the "mode" or the "type of said monitoring function." Finally, the Examiner fails to provide the required "analysis" which would support his combination disclosures taken from the Alverson/Angelo combination.

As a result of the above, there is simply no support for the rejections of Appellants' independent claim or claims dependent thereon under 35 USC §103. Thus, and in view of the above, the rejection of claims 1, 2, 4-21 and 23-39 under 35 USC §103 is clearly in error and reversal thereof by this Honorable Board is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
Enclosures

IX. CLAIMS APPENDIX

1. A method of controlling a monitoring function of a processor, said processor being operable in at least two domains, comprising a first domain and a second domain, said first and second domains each comprising at least one mode, said method comprising the steps of:

controllably monitoring said processor operating in each of said at least two domains,

setting at least one control value to an enable value, said at least one control value relating to a condition, said condition consisting of a respective one of (a) a domain that said processor is operating in, or (b) a mode that said processor is operating in or (c) a type of said monitoring function, said control value being set to be an enable value for said related condition to indicate that said monitoring function is allowable in said first domain;

allowing initiation of said monitoring function in said first domain when said condition is present if its related control value is set to said enable value and thereby indicates that said monitoring function is allowable; and

not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value is not set to said enable value and thereby indicates that said monitoring function is not allowable.

2. A method according to claim 1, wherein said first domain is a secure domain and said second domain is a non-secure domain, said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain.

4. A method according to claim 2, wherein said condition comprises a secure domain and said control value comprises a secure domain enable value, initiation of monitoring in said secure domain only being allowed if said secure domain enable value is set.

5. A method according to claim 2, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode.

6. A method according to claim 5 wherein said control value comprises a secure user mode enable bit and initiation of monitoring from secure user mode is only allowed if said secure user mode enable bit has been set.

7. A method according to claim 4, wherein said condition comprises a type of monitoring function.

8. A method according to claim 7, wherein said condition comprises a debug monitoring function and said control value comprises a debug enable bit, initiation of debug in said first domain only being allowable if said debug enable bit has been set.

9. A method according to claim 8, wherein said condition comprises a trace monitoring function and said control value comprises a trace enable bit, initiation of trace in said first domain only being allowable if said control trace enable bit has been set.

10. A method according to claim 9, wherein said secure domain enable value comprises a secure debug enable bit and a secure trace enable bit, initiation of debug and trace in said secure domain only being allowable if respective portions of said secure domain enable value are set.

11. A method according to claim 1, said method comprising setting a plurality of control values, each of said plurality of control values relating to a different condition; and

only allowing initiation of said monitoring function in said first domain if any of said conditions are present if each of said control values related to a condition that is present indicate that said monitoring function is allowable.

12. A method according to claim 1, said method further comprising said steps of:

setting a control indicator, said control indicator indicating that monitoring is only allowable for specified applications; and

prior to initialising said monitoring function checking an application identifier; and

only allowing initiation of said monitoring function if said application currently running is one for which monitoring is allowable.

13. A method according to claim 12, wherein the step of setting a control indicator comprises setting a control indicator stored in a predetermined position in a storage element.

14. A method according to claim 12, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data, said method comprising the further step of:

following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain while an application running on said processor is one for which monitoring is allowable.

15. A method according to claim 1, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data, said method comprising the further step of:

following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain when a condition changes if a control value related to the changed condition indicates that said monitoring function is allowable.

16. A method according to claim 1, wherein setting of at least one control value is performed either by setting said control value via an input port or by setting said control value from the first domain.

17. A method according to claim 16, said method comprising the further step of blocking write access to said control value via said input port such that the step of setting said control value can henceforth only be performed by setting said control value from said first domain.

18. A method according to claim 1, wherein said first domain comprises a first user mode and a first privileged mode and the step of setting at least one control value in said first domain, comprises setting said control value from said first privileged mode.

19. A method according to claim 16, wherein said first domain comprises a first user mode and a first privileged mode and said step of setting at least one control value in the first domain, comprises inputting an authentication code from a mode that is not a first privileged mode and then setting said control value.

20. A processor operable in a first domain and a second domain said first and second domains each comprising at least one mode, said processor comprising:

monitoring logic for controllably monitoring said processor operating in each of said first and second domains;

a storage element configured to be set to contain at least one control value, said at least one control value relating to a condition, said condition consisting of a respective one of (a) a domain that said processor is operating in, or (b) a mode that said processor is operating in or (c) a type of said monitoring function, said control value comprising an enable value for said related condition, said enable

value indicating that operation of said monitoring logic is allowable in said first domain; and

control logic configured to control initiation of said monitoring logic and for allowing initiation of said monitoring logic in said first domain when said condition is present if its related control value is set to said enable value and thereby indicates that operation of said monitoring logic is allowable, and for not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value is not set to said enable value and thereby indicates that operation of said monitoring logic is not allowable.

21. A processor according to claim 20, wherein said first domain is a secure domain and said second domain is a non-secure domain said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain.

23. A processor according to claim 21, wherein said condition comprises a secure domain and said control value comprises a secure domain enable bit, initiation of monitoring in said secure domain only being allowed if said storage element contains a secure domain enable bit.

24. A processor according to claim 21, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode.

25. A processor according to claim 24 wherein said control value comprises a secure user mode enable bit and said control logic is operable to allow initiation of said monitoring logic from secure user mode only when said storage element contains a secure user mode enable bit.

26. A processor according to claim 21, wherein said condition comprises a type of monitoring function.

27. A processor according to claim 26, wherein said condition comprises debug monitoring and the control value comprises a debug enable bit, said control logic being operable to allow initiation of said monitoring logic in said first domain only when the storage element contains a debug enable bit.

28. A processor according to claim 26, wherein said condition comprises trace monitoring and said control value comprises a trace enable bit, said control logic being operable to allow initiation of said trace logic in said first domain only when said storage element contains a control trace enable bit.

29. A processor according to claim 20, wherein:

said storage element is operable to contain a plurality of control values, each of said plurality of control values relating to a different condition; and

said control logic is operable to only allow initiation of said monitoring logic in said first domain if any of said conditions are present if each of the control values related to a condition that is present indicate that the monitoring logic is allowable.

30. A processor according to claim 29 wherein one condition comprises a secure domain and a corresponding control value comprises a secure domain enable bit and a further condition comprises a secure user mode and a corresponding control value comprises a secure user mode enable bit, said control logic being operable to initiate said monitoring logic from secure user mode only when said storage element contains both a secure user mode enable bit and a secure domain enable bit.

31. A processor according to claim 20, wherein:

said storage element is further operable to contain a control indicator, said control indicator indicating that monitoring is only allowable for identified applications; and

said control logic is operable to check at least one identifier identifying an application that is allowable, said control logic only initiating said monitoring logic in the first domain when said application currently running is one identified as being one for which monitoring is allowable.

32. A processor according to claim 31, said processor comprising a further storage element, said storage element being operable to contain said at least one identifier specifying an application that is allowable.

33. A processor according to claim 31, wherein said monitoring logic is operable to monitor the processor and capture diagnostic data; and

wherein said control logic is operable to control the monitoring logic to suppress capturing of diagnostic data in said first domain when said control logic detects that said application running is not one identified as being allowable.

34. A processor according to claim 20, said processor further comprising an input port, wherein said control value is operable to be set in said storage element either via the input port or via an input from said first domain.

35. A processor according to claim 34, said processor comprising a means of blocking write access to said control value via said input port such that setting

of said control value can henceforth only be performed by setting said control value via an input from said first domain.

36. A processor according to claim 20, wherein said first domain comprises a first user mode and a first privileged mode and said control value is operable to be set in said storage element via an input from said first privileged mode.

37. A processor according to claim 35, wherein said first domain comprises a first user mode and a first privileged mode and said control value is operable to be set in said storage element by input of an authentication code from a mode that is not a first privileged mode followed by an input of said control value.

38. A processor according to claim 20, wherein said storage element comprises a register.

39. A processor according to claim 30, wherein said further storage element comprises a register.

X. EVIDENCE APPENDIX

Page 762 from *Webster's Ninth New Collegiate Dictionary*.

XI. RELATED PROCEEDINGS APPENDIX

BPAI Decision dated March 31, 2010 in Appeal No. 2008-5801.

²mob *vt* **mobbed; mob·bing** (1709) 1 : to crowd about and attack or annoy ⟨*mobbed* by autograph hunters before he could enter the theater⟩ 2 : to crowd into or around ⟨customers ~ the stores on sale days⟩

mob·cap \'mäb-ˌkap\ *n* [*mob* (woman's cap) + *cap*] (1795) : a woman's fancy indoor cap made with a high full crown and often tied under the chin

¹mo·bile \'mō-bəl, -ˌbēl, -ˌbīl\ *adj* [MF, fr. L *mobilis*, fr. *movēre* to move] (15c) 1 : capable of moving or being moved : MOVABLE ⟨a ~ missile launcher⟩ 2 a : changeable in appearance, mood, or purpose ⟨~ face⟩ b : ADAPTABLE, VERSATILE 3 : MIGRATORY 4 a : characterized by the mixing of social groups b : having the opportunity for or undergoing a shift in status within the hierarchical social levels of a society ⟨upwardly ~ workers⟩ 5 : marked by the use of vehicles for transportation ⟨~ warfare⟩ 6 : of or relating to a mobile — **mo·bil·i·ty** \mō-'bil-ət-ē\ *n*

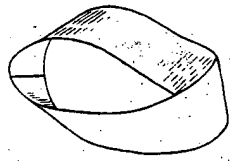
²mo·bile \'mō-ˌbēl\ *n* (1936) : a construction or sculpture frequently of wire and sheet metal shapes with parts that can be set in motion by air currents; *also* : a similar structure (as of paper or plastic) suspended so that it moves in a current of air

mobile home *n* (1949) : a trailer that is used as a permanent dwelling, is usu. connected to utilities, and is designed without a permanent foundation — compare MOTOR HOME

mo·bi·li·za·tion \ˌmō-bə-lə-'zā-shən\ *n* (1799) 1 : the act of mobilizing 2 : the state of being mobilized

mo·bi·lize \'mō-bəˌlīz\ *vb* **-lized; -liz·ing** *vt* (1838) 1 a : to put into movement or circulation ⟨~ financial assets⟩ b : to release (something stored in the organism) for bodily use 2 a : to assemble and make ready for war duty b : to marshal (as resources) for action ⟨~ support for a proposal⟩ ~ *vi* : to undergo mobilization

Mö·bi·us strip \ˌmōˑ-bē-əs-, ˌmə(r)-, ˌmō-\ *n* [August F. *Möbius* †1868 Ger. mathematician] (1904) : a one-sided surface that is constructed from a rectangle by holding one end fixed, rotating the opposite end through 180 degrees, and applying it to the first end



Möbius strip

mob·oc·ra·cy \mä-'bäk-rə-sē\ *n* (1754) 1 : rule by the mob 2 : the mob as a ruling class — **mob·ocrat** \'mäb-əˌkrat\ *n* — **mob·ocrat·ic** \ˌmäb-ə-'krat-ik\ *adj*

mob·ster \'mäb-stər\ *n* (1917) : a member of a criminal gang

moc·ca·sin \'mäk-ə-sən\ *n* [of Algonquian origin; akin to Natick *mokkussin* shoe] (1612) 1 a : a soft leather heelless shoe or boot with the sole brought up the sides of the foot and over the toes where it is joined with a puckered seam to a U-shaped piece lying on top of the foot b : a regular shoe having a seam on the forepart of the vamp imitating the seam of a moccasin 2 a : WATER MOCCASIN b : a snake (as of the genus *Natrix*) resembling a water moccasin

moccasin flower *n* (1680) : any of several lady's slippers (genus *Cypripedium*); *esp* : a once common woodland orchid (*C. acaule*) of eastern No. America with pink or white moccasin-shaped flowers

mo·cha \'mō-kə\ *n* [*Mocha*, Arabia] (1773) 1 a (1) : a superior Arabian coffee consisting of small green or yellowish beans (2) : a coffee of superior quality b : a flavoring made of a strong coffee infusion or of a mixture of cocoa or chocolate with coffee 2 : a pliable suede-finished glove leather from African sheepskins

¹mock \'mäk, 'mók\ *vb* [ME *mocken*, fr. MF *mocquer*] *vt* (15c) 1 : to treat with contempt or ridicule : DERIDE 2 : to disappoint the hopes of : DELUDE 3 : DEFY, CHALLENGE 4 a : to imitate (as a sound or mannerism) closely : MIMIC b : to mimic in sport or derision ~ *vi* : JEER, SCOFF *syn* see RIDICULE, COPY — **mock·er** *n* — **mock·ing·ly** \-iŋ-lē\ *adv*

²mock *n* (15c) 1 : an act of ridicule or derision : JEER 2 : one that is an object of derision or scorn 3 : MOCKERY 4 a : an act of imitation b : something made as an imitation

³mock *adj* (1548) : of, relating to, or having the character of an imitation : SIMULATED, FEIGNED ⟨the ~ solemnity of the parody⟩

⁴mock *adv* (1619) : in an insincere or counterfeit manner — usu. used in combination ⟨*mock*-serious⟩

mock·ery \'mäk-(ə-)rē, 'mók-\ *n, pl* **-er·ies** (15c) 1 : insulting or contemptuous action or speech : DERISION 2 : a subject of laughter, derision, or sport 3 a : a counterfeit appearance : IMITATION b : an insincere, contemptible, or impertinent imitation ⟨arbitrary methods that make a ~ of justice⟩ 4 : something ridiculously or impudently unsuitable

¹mock–he·ro·ic \ˌmäk-hi-'rō-ik, ˌmók-\ *adj* (ca. 1711) : ridiculing or burlesquing heroic style, character, or action ⟨a ~ poem⟩ — **mock–he·ro·ical·ly** \-i-k(ə-)lē\ *adv*

²mock–heroic *n* (1728) : a mock-heroic composition — called also *mock-epic*

mock·ing·bird \'mäk-iŋ-ˌbərd, 'mók-\ *n* (1676) : a common bird (*Mimus polyglottos*) esp. of the southern U.S. that is remarkable for its exact imitations of the notes of other birds

mock orange *n* (1731) : any of various usu. shrubby plants considered to resemble the orange; *esp* : PHILADELPHUS

mock turtle soup *n* (1783) : a soup made of meat (as calf's head or veal), wine, and spices in imitation of green turtle soup

mock–up \'mäk-ˌəp, 'mók-\ *n* (1920) : a full-sized structural model built accurately to scale chiefly for study, testing, or display

¹mod \'mäd\ *adj* (1964) : MODERN; *esp* : bold and free in style, behavior, or dress

²mod *n* (1965) : one who wears mod clothes

mod·acryl·ic fiber \ˌmäd-ə-ˌkril-ik-\ *n* [*modified acrylic*] (1960) : any of various synthetic textile fibers that are long-chain polymers composed of 35 to 85 percent by weight of acrylonitrile units

mod·al \'mōd-ᵊl\ *adj* [ML *modalis*, fr. L *modus*] (1569) 1 : of or relating to modality in logic 2 : containing provisions as to the mode of procedure or the manner of taking effect — used of a contract or legacy 3 : of or relating to a musical mode 4 : of or relating to structure as opposed to substance 5 : of, relating to, or constituting a grammatical form or category characteristically indicating predication of an action or state in some manner other than as a simple fact 6 : of or relating to a statistical mode — **mod·al·ly** \-ᵊl-ē\ *adv*

modal auxiliary *n* (ca. 1904) : an auxiliary verb (as *can, must, might, may*) that is characteristically used with a verb of predication and expresses a modal modification and that in English differs formally from other verbs in lacking *-s* and *-ing* forms

mo·dal·i·ty \mō-'dal-ət-ē\ *n, pl* **-ties** (1617) 1 a : the quality or state of being modal b : a modal quality or attribute : FORM 2 : the classification of logical propositions according to their asserting or denying the possibility, impossibility, contingency, or necessity of their content 3 : one of the main avenues of sensation (as vision) 4 : a usu. physical therapeutic agency

¹mode \'mōd\ *n* [ME *moede*, fr. L *modus* measure, manner, musical mode — more at METE] (14c) 1 a : an arrangement of the eight diatonic notes or tones of an octave according to one of several fixed schemes of their intervals b : a rhythmical scheme (as in 13th and 14th century music) 2 : ²MOOD 2 3 [LL *modus*, fr. L] a : ²MOOD 1 b : the modal form of the assertion or denial of a logical proposition 4 a : a particular form or variety of something b : a form or manner of expression : STYLE 5 : a possible, customary, or preferred way of doing something (explained in the usual solemn ~) 6 a : a manifestation, form, or arrangement of being; *specif* : a particular form or manifestation of an underlying substance b : a particular functioning arrangement or condition : STATUS ⟨a spacecraft in reentry ~⟩ ⟨a computer operating in parallel ~⟩ 7 a : the most frequent value of a set of data b : a value of a random variable for which a function of probabilities defined on it achieves a relative maximum 8 : any of various stationary vibration patterns of which an elastic body or oscillatory system is capable ⟨the vibration ~ of an airplane propeller blade⟩ ⟨the ~s of electromagnetic radiation in a waveguide⟩ 9 : the actual mineral composition of a rock *syn* see METHOD

²mode *n* [F, fr. L *modus*] (1645) : a prevailing fashion or style (as of dress or behavior) *syn* see FASHION

¹mod·el \'mäd-ᵊl\ *n* [MF *modelle*, fr. OIt *modello*, fr. (assumed) VL *modellus*, fr. L *modulus* small measure, fr. *modus*] (1575) 1 *obs* : a set of plans for a building 2 *dial Brit* : COPY, IMAGE 3 : structural design ⟨a home on the ~ of an old farmhouse⟩ 4 : a miniature representation of something; *also* : a pattern of something to be made 5 : an example for imitation or emulation 6 : a person or thing that serves as a pattern for an artist; *esp* : one who poses for an artist 7 : ARCHETYPE 8 : an organism whose appearance a mimic imitates 9 : one who is employed to display clothes or other merchandise : MANNEQUIN 10 a : a type or design of clothing b : a type or design of product (as a car or airplane) 11 : a description or analogy used to help visualize something (as an atom) that cannot be directly observed 12 : a system of postulates, data, and inferences presented as a mathematical description of an entity or state of affairs

syn MODEL, EXAMPLE, PATTERN, EXEMPLAR, IDEAL mean someone or something set before one for guidance or imitation. MODEL applies to something taken or proposed as worthy of imitation: EXAMPLE applies to a person to be imitated or in some contexts on no account to be imitated but to be regarded as a warning; PATTERN suggests a clear and detailed archetype or prototype; EXEMPLAR suggests either a faultless example to be emulated or a perfect typification; IDEAL implies the best possible exemplification either in reality or in conception.

²model *vb* **mod·eled** *or* **mod·elled; mod·el·ing** *or* **mod·el·ling** \'mäd-liŋ, -ᵊl-iŋ\ *vt* (1730) 1 : to plan or form after a pattern : SHAPE 2 *archaic* : to make into an organization (as an army, government, or parish) 3 a : to shape or fashion in a plastic material b : to produce a representation or simulation of ⟨using a computer to ~ a problem⟩ 4 : to construct or fashion in imitation of a particular model ⟨~*ed* its constitution on that of the U.S.⟩ 5 : to display by wearing, using, or posing with ⟨~*ed* gowns⟩ ~ *vi* 1 : to design or imitate forms : make a pattern ⟨enjoys ~*ing* in clay⟩ 2 : to work or act as a fashion model — **mod·el·er** \'mäd-lər, -ᵊl-ər\ *n*

³model *adj* (1844) 1 : serving as or capable of serving as a pattern ⟨a ~ student⟩ 2 : being a miniature representation of something ⟨a ~ airplane⟩

mo·dem \'mō-ˌdem\ *n* [*mo*dulator + *dem*odulator] (ca. 1952) : a device that converts signals from one form to a form compatible with another kind of equipment ⟨a ~ for transmitting computer data over telephone lines⟩

¹mod·er·ate \'mäd-(ə-)rət\ *adj* [ME, fr. L *moderatus*, fr. pp. of *moderare* to moderate; akin to L *modus* measure] (15c) 1 a : avoiding extremes of behavior or expression : observing reasonable limits ⟨a ~ drinker⟩ b : CALM, TEMPERATE 2 a : tending toward the mean or average amount or dimension b : having average or less than average quality : MEDIOCRE 3 : avoiding extreme political or social measures ⟨a ~ candidate⟩ 4 : limited in scope or effect 5 : not expensive : reasonable or low in price 6 *of a color* : of medium lightness and medium chroma — **mod·er·ate·ly** *adv* — **mod·er·ate·ness** *n*

²mod·er·ate \'mäd-əˌrāt\ *vb* **-at·ed; -at·ing** *vt* (15c) 1 : to lessen the intensity or extremeness of ⟨the sun *moderated* the chill⟩ 2 : to preside over or act as chairman of ~ *vi* 1 : to act as a moderator 2 : to become less violent, severe, or intense — **mod·er·a·tion** \ˌmäd-ə-'rā-shən\ *n*

³mod·er·ate \'mäd-(ə-)rət\ *n* (1794) : one who holds moderate views or who belongs to a group favoring a moderate course or program (as in politics or religion)

moderate breeze *n* (ca. 1805) : wind having a speed of 13 to 18 miles per hour

moderate gale *n* (ca. 1805) : wind having a speed of 32 to 38 miles per hour

mo·der·a·to \ˌmäd-ə-'rät-(ˌ)ō\ *adv or adj* [It, fr. L *moderatus*] (ca. 1724) : MODERATE — used as a direction in music to indicate tempo

mod·er·a·tor \'mäd-əˌrāt-ər\ *n* (1560) 1 : one who arbitrates : MEDIATOR 2 : one who presides over an assembly, meeting, or discussion: as a : the presiding officer of a Presbyterian governing body b : the nonpartisan presiding officer of a town meeting c : the chairman of a discussion group 3 : a substance (as graphite) used for slowing down neutrons in a nuclear reactor — **mod·er·a·tor·ship** \-ˌship\ *n*

¹mod·ern \'mäd-ərn, ÷'mäd-(ə-)rən\ *adj* [LL *modernus*, fr. L *modo* just now, fr. *modus* measure — more at METE] (1585) 1 a : of, relating to, or characteristic of a period extending from a relevant remote past to the present time b : of, relating to, or characteristic of the present or the immediate past : CONTEMPORARY 2 : involving recent techniques,

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,483	11/17/2003	Simon Charles Watt	550-471	6434

23117 7590 03/31/2009
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
JOHNSON, BRIAN P	

ART UNIT	PAPER NUMBER
2183	

MAIL DATE	DELIVERY MODE
03/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SIMON CHARLES WATT and LUC ORION

Appeal 2008-5801
Application 10/714,483
Technology Center 2100

Decided:[1] March 31, 2009

Before HOWARD B. BLANKENSHIP, JAY P. LUCAS, and THU A. DANG, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-39, which are all the pending claims. We have jurisdiction under 35 U.S.C. § 6(b). Oral argument by Appellants' representative was heard on March 18, 2009.

We affirm.

Invention

Appellants' invention relates to a method of controlling a monitoring function of a processor that is operable in at least two (e.g., secure and less secure) domains. (*See* Abstract.)

Representative Claim

1. A method of controlling a monitoring function of a processor, said processor being operable in at least two domains, comprising a first domain and a second domain, said first and second domains each comprising at least one mode, said method comprising the steps of:

controllably monitoring said processor operating in each of said at least two domains,

setting at least one control value, said at least one control value relating to a condition and being indicative of whether said monitoring function is allowable in said first domain;

allowing initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that said monitoring function is allowable; and

not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value indicates that said monitoring function is not allowable.

Prior Art

The Examiner relies on the following references as evidence of unpatentability.

Christensen	US 5,752,013	May 12, 1998
Angelo	US 6,581,162 B1	Jun. 17, 2003
Faccin	US 6,879,690 B2	Apr. 12, 2005
Alverson	US 7,020,767 B2	Mar. 28, 2006

Examiner's Rejections

Claims 1-8, 11-16, 18-36, 38, and 39 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Alverson and Angelo.[2]

Claims 9, 10, 17, and 37 stand rejected under 35 U.S.C. § 103(a) over Alverson, Angelo, and "common art."

[2] The Answer (at 3) erroneously lists claim 10, which depends from claim 9, as being unpatentable over the first-stated combination.

Claim Groupings

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal on the basis of claims 1, 9, and 20. See 37 C.F.R. § 41.37(c)(1)(vii).

FINDINGS OF FACT

Angelo

1. Angelo describes a secure environment for entering and storing information necessary for encryption processes, using the secure memory space provided by System Management Mode (SMM) memory. Angelo Abstract.

2. According to Angelo, SMM is entered upon receipt of a system management interrupt (SMI). Conventionally, SMIs were used for power management in portable systems. Angelo col. 7, ll. 40-55.

3. SMIs are asserted by an SMI timer, by a system request, or by other means. *Id.*, ll. 56-57.

4. An SMI is a non-maskable interrupt of very high priority. Only the reset signal and the cache flush signal have higher priority. *Id.*, ll. 57-61.

5. When an SMI is asserted, a microprocessor maps SMM memory into the main memory space. The entire CPU state is saved in SMM memory, after which an SMI handler routine services the interrupt. *Id.*, col. 7, l. 61 - col. 8, l. 4.

6. While the SMI handler routine is executing, other interrupt requests are not serviced, but ignored. *Id.*, col. 8, ll. 4-7.

7. The SMI handler can be written to perform tasks other than the original power management tasks. Because SMM memory is only addressable while the computer system is in SM mode, critical information entered into the memory is secure. *Id.*, col. 8, ll. 39-52.

8. Angelo discusses a procedure (Fig. 5) for securely obtaining a single character from the keyboard to placement in secure memory. A request for secure keyboard communications causes the computer's processor to enter into SMM, so that the SMI handler can ensure that entered data is stored in secure memory. *Id.*, ll. 53-66.

9. The procedure of Figure 5 may begin when the computer system detects a request for secure communications. *Id.*, col. 9, ll. 3-6.

10. Control proceeds to step 402 (Fig. 5), where appropriate registers in the processor are loaded prior to execution of the SMI code. *Id.*, ll. 6-8.

11. The register values indicate a request for secured keyboard communications. *Id.*, ll. 8-9.

12. Control proceeds to step 404 (Fig. 5), where an application generates a "soft" SMI (a software interrupt), which places the processor in SMM. *Id.*, ll. 9-13.

13. The processor executes the SMI handler routine. *Id.*, ll. 22-24.

14. The SMI handler examines the processor registers to determine what type of process (e.g., secure keyboard request) initiated the request, and performs accordingly. *Id.*, ll. 24-29.

15. One skilled in the art would have understood that, when the processor register values indicate that an SMI should be generated (FF 11, 12), SMM may be entered (FF 12), but would not be entered when an interrupt of higher priority (e.g., FF 4) is present.

16. One skilled in the art would have known that the processor also handles other system requests, in addition to the SM interrupt.

PRINCIPLES OF LAW

A person having ordinary skill in the art uses known elements for their intended purpose. *Anderson's-Black Rock, Inc. v. Pavement Salvage Co.*, 396 U.S. 57 (1969) (radiant-heat burner used for its intended purpose in combination with a spreader and a tamper and screed).

"[W]hen a patent 'simply arranges old elements with each performing the same function it had been known to perform' and yields no more than one would expect from such an arrangement, the combination is obvious." *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1740 (2007) (quoting *Sakraida v. Ag Pro, Inc.*, 425 U.S. 273, 282 (1976)).

ANALYSIS

The Examiner finds that the SMI taught by Angelo corresponds to the "control value" recited in instant claim 1. Appellants acknowledge (App. Br. 10) that entry into the SMM as taught by Angelo is a "monitoring function." (*See also* Ans. 15.) However, Appellants allege that the function is always allowed in response to an SMI. (App. Br. 10.)

Although Appellants' allegation is irrelevant to the rejection, the allegation is unfounded. Angelo teaches that the function is usually, *but not always*, allowed in response to an SMI. (*See* FF 15).

The Examiner further finds that the control value (SMI interrupt) is related to several "conditions" that meet the terms of instant claim 1. (Ans. 14; *see* FF 3.) Appellants allege that the term "condition" has some (unidentified) special meaning in the art (Reply Br. 2), but do not refer us to any evidence in support of the allegation, nor tell us what that the unsupported, unidentified special meaning may be. Appellants also refer to a "number of embodiments" in the Specification and seem to assert that some (unidentified) special meaning of "condition" can be gleaned from the described embodiments (*see id.*), which, presumably, would distinguish over the conditions in Angelo that were identified by the Examiner. Thus, although Appellants allege (*id.*) there is a "definition" for the term "condition" set out in the Specification, Appellants not only do not tell us where the definition may be found, but also neglect to tell us what that the definition may be.

We will not, and cannot, read any of the specific embodiments described in the Specification into instant claim 1. The *claims* measure the invention. *See SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). Our reviewing court has repeatedly warned against confining the claims to specific embodiments described in the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc). During prosecution before the USPTO, claims are to be given their broadest reasonable interpretation, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997); *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404-05 (CCPA 1969). "An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed, as much as possible, during the administrative process." *In re Zletz*, 893 F.2d at 322.

In any event, the Examiner finds that one of the "conditions" taught by Angelo is a system request. (Ans. 14.) Angelo describes a secure user mode (FF 8-14). Register values in the processor are loaded to indicate the condition of the secure user mode (FF 10-11). A system request, in response to the request for secure user mode, subsequently generates an interrupt (asserts the SMI) and enters the system into SM mode (FF 12).

However, other interrupt requests, in addition to the SMI, are serviced by the processor (FF 6, 16). Angelo thus teaches allowing initiation of the

monitoring function in the first domain when the condition (system request) is present if its related control value indicates that the monitoring function is allowable (system request to assert SMI; SMI is asserted), and not allowing initiation of the monitoring function in the first domain when the condition (system request) is present and its related control value indicates that the monitoring function is not allowable (system request to assert some other interrupt; SMI not asserted).

Appellants' claim 1 sets no limitation on the substance of the "control value," but provides some kind of abstract, sideways definition by reference to what the value may be "relating to" or "indicative of." In claim 1, the "control value" is "indicative of" only two states -- allowable or not allowable. The claimed "control value" can be a signal level, as Appellants seem to acknowledge at pages 3 and 4 of the Reply Brief. However, the "control value" can also be an element in a processor register that causes the signal level to be asserted (FF 10-11), or an element in program memory that causes the application to generate the particular (SMI) software interrupt (*see* FF 12).

With respect to claim 20, Appellants argue that Angelo does not teach a "storage element" operable to be set to contain at least one control value. (App. Br. 6-7.) We disagree. (*See* FF 10-12.) Angelo teaches a "storage element" --registers in the processor -- operable to be set to contain at least one control value -- one or more bits that indicate an SM interrupt is to be asserted.

Appellants also allege (App. Br. 9) that the Examiner has not shown where the "not allowing" step of claim 1 or the "control logic" of claim 20 is taught by the references. In Appellants' only response to more specific findings set out by the Examiner (Ans. 16-17), Appellants repeat the allegation that Angelo teaches the "direct opposite," or is "diametrically opposite," to what is specified in Appellants' claims. (Reply Br. 6.) Appellants' remarks are not persuasive of error in the rejection of claim 1 or claim 20, because Appellants have not shown that Angelo teaches anything "opposite" to what is claimed.

With respect to the rejection of claim 9 over Alverson, Angelo, and "common art," the "common art" takes the form of official notice that "saving instruction traces is [sic; was] common in the art and can be utilized for many debugging purposes." (Final Rej. 11; Ans. 12.)

Appellants contend they have "traversed" the Examiner's taking of official notice. (App. Br. 11, 13.) However, the "traversal" consists of pointing out that the Examiner failed to cite any supporting evidence. (*See* App. Br. 11.) Appellants' "traversal" thus takes the form of pointing out that the official notice is official notice.

The USPTO may take notice of facts beyond the record which, while not generally notorious, are capable of instant and unquestionable demonstration as to defy dispute. *In re Ahlert*, 424 F.2d 1088, 1091 (CCPA 1970). In the instant case, Appellants have not traversed the Examiner's official notice. A "traverse" is not pointing out that the Examiner has not

provided supporting evidence for the official notice. Nor is a "traverse" a demand for evidence. A "traverse" is a denial of an opposing party's allegations of fact. *See Black's Law Dictionary Fifth Edition* ("In common law pleading, a traverse signifies a denial."). Moreover, an *adequate* traverse must contain adequate information or argument to create on its face a reasonable doubt regarding the circumstances justifying the official notice. *In re Boon*, 439 F.2d 724, 728 (CCPA 1971).

In response to Appellants' concerns, although under no obligation to do so, the Examiner cited two prior art patents in support of the official notice. (Ans. 18.) Appellants do not deny that saving instruction traces was common in the art and could be utilized for many debugging purposes (*see* App. Br. 11; Reply Br. 7-8). Nor do Appellants assert that the Examiner's cited evidence fails to support the official notice (*see* Reply Br. 7-8). Appellants merely submit that the Examiner "must provide some 'rationale' or 'motivation' for combining those new references with the Alverson/Angelo combination." (Reply Br. 8.)

We disagree that the Examiner must provide some "rationale" or "motivation" for combining the newly cited references with Alverson and Angelo. The Examiner finds that the artisan would have been motivated to use the known technique of saving instruction traces to gather more debugging or security information for analysis. (App. Br. 12.) The Examiner further finds that it would have been obvious to one of ordinary skill in the art to include a trace enable bit to indicate to the processor that

instruction traces are to be saved. (*Id.*) Appellants have done nothing to call these findings into question, nor alleged that the proposed combination would not result in the claimed invention other than, perhaps, the alleged lack of "relating to" and "indicative of" that we have previously considered.

Finally, Appellants allege that "at no point in the rejection" does the Examiner provide the required "reason" or "motivation" for combining the Alverson and Angelo references. (App. Br. 12.) However, the Examiner finds that, with the knowledge evidenced by Alverson and Angelo, the ordinary artisan would have been motivated to use the techniques taught by Angelo in computer security memory management, with domain-specific multiple levels of protection. (Ans. 3.)

Appellants submit in response that "Alverson has no suggestion that combining it with portions of Angelo or other references would provide any benefit at all if or when portions where [sic] combined with portions of Alverson." (Reply Br. 9.) Appellants do not allege that anything about the proposed combination might be deficient, other than the lack of specific suggestion in one reference or the other for the combination (*see* Reply Br. 8-10).

Presumably, Appellants know there is no requirement that one reference provide a specific suggestion to combine some elements with some other elements in another reference. Appellants seem to submit the remarks in response to the Examiner's reference to what, for example, "Alverson" would have been motivated to do (*see* Ans. 3). However,

Appellants could not have been misled into the belief that the rejection is based on what would have been obvious to some unidentified entity (e.g., "Alverson"), because the rejection is under 35 U.S.C. § 103. The statute is specific with respect to what would have been obvious "to a person having ordinary skill in the art."

Thus, for the claims we have reviewed, Appellants have not shown that the invention does anything more than simply arrange old elements with each performing the same function it had been known to perform, yielding no more than one would expect from such an arrangement, and thus an obvious combination. *See KSR* at 1740.

We have considered all of Appellants' arguments in response to the rejections. We are not persuaded that any of the claims have been rejected in error. We sustain the § 103(a) rejections of claims 1-39.

DECISION

The rejection of claims 1-8, 11-16, 18-36, 38, and 39 under 35 U.S.C. § 103(a) as being unpatentable over Alverson and Angelo is affirmed.

The rejection of claims 9, 10, 17, and 37 under 35 U.S.C. § 103(a) over Alverson, Angelo, and "common art" is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

rwk

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON VA 22203